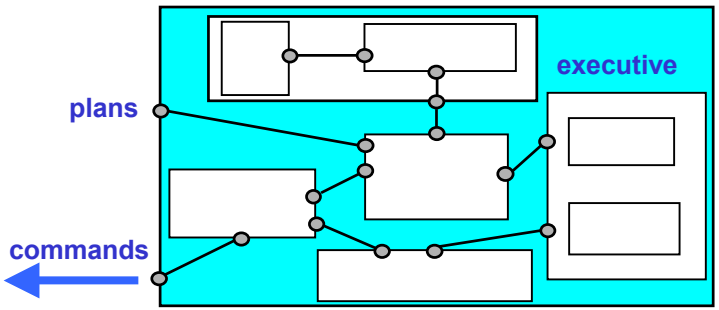
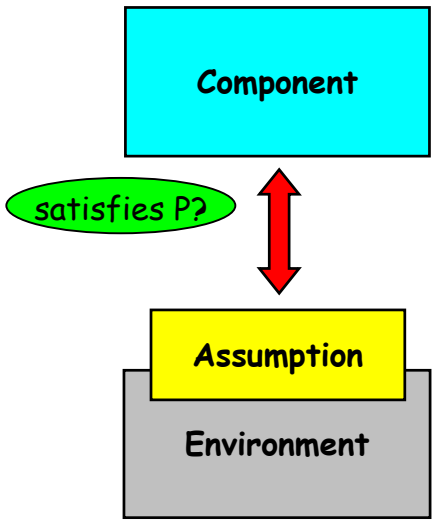
Presentation on System-Level Verification for Autonomous Systems: Automatic Assumption Generation for Component Verification

Information Science & Technology
Ames Research Center



Microsoft
Microsoft Research



Intelligent Systems Program: System-level verification for autonomy software

- Verification is essential for autonomy insertion in missions

Objectives

- Provide support for component-based verification (scalability)

Approach

- Component verification with automatically generated assumptions

Two novel solutions developed at NASA Ames

1. Algorithmic generation of assumptions; knowledge of environment **is not** required
2. **Incremental** assumption computation based on counterexamples, learning and knowledge of environment

Explanation

- **POC:** Dimitra Giannakopoulou and Corina Păsăreanu

- **Shown on slide:** One of the objectives of the Intelligent Systems project on "System-Level Verification Technology for Autonomy Software" is to provide support for component-based verification, to improve scalability. A common approach to component-based verification involves assume-guarantee reasoning and makes use of "assumptions," i.e., abstractions of the environment of a system component. Although aimed at scalability, such reasoning has not been widely applied, because coming up with appropriate assumptions is a difficult manual process. Two novel techniques were developed at NASA Ames for generating assumptions automatically. The first technique synthesizes the weakest assumption that a component needs to make about its environment for a given property to be satisfied. The second technique defines a framework for incremental, and fully automated assume-guarantee reasoning, based on learning. Both techniques have been successfully applied to a number of NASA case studies.

- **Accomplishment:** Dimitra Giannakopoulou and Corina Păsăreanu visited Microsoft Research in Redmond, at the invitation of Shaz Qadeer. They gave a two hour presentation on the recent work on assumption generation that was done in the context of the IS project. They had extensive discussions with members of the Software Productivity Tools and the AsmL groups at MSR.